AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claims 1-13 (Canceled)

Claim 14 (New): An application authentication system comprising:

a terminal device on which an application is operated; and

a secure device connected fixedly or detachably to the terminal device,

wherein the terminal device includes:

application recording unit configured to record the application which is operated on the terminal device and performs processing using data held by the secure device; and

application running unit configured to run the application,

wherein the secure device includes:

data holding unit configured to hold the data used by the application which is operated on the terminal device;

verifying unit configured to verify validity of the application running means and validity of the application; and

accepting unit configured to accept access from the application to the data held in the data holding means when the validities of the application running means and the application are authenticated,

wherein the application running means calculates digest data of the application and sends the digest data to the verifying means after the validity of the application running means is authenticated by the verifying means, and

wherein the verifying means verifies the validity of the application using the transmitted digest data.

Claim 15 (New): A secure device connected fixedly or detachably to a terminal which includes application running unit configured to run an application, the secure device comprising:

data holding unit configured to hold data used by the application;

verifying unit configured to verify validity of the application running means and validity of the application; and

accepting unit configured to accept access from the application to the data held in the data holding means when the validities of the application running means and the application are authenticated,

wherein the application running means of the terminal calculates digest data of the application and sends the digest data to the verifying means after the validity of the application running means is authenticated by the verifying means, and

wherein the verifying means verifies the validity of the application using the transmitted digest data.

Claim 16 (New): The secure device according to claim 15, wherein

an electronic signature is attached to the application by a certificate authority,

the application running means transmits the electronic signature attached to the application to the secure device,

the verifying means verifies the electronic signature by using a pubic key of the certificate authority and the digest data, and authenticates the application when a result of the verification is normal.

Claim 17 (New): The secure device according to claim 15, wherein the verifying means holds the digest data of the application in advance, collates the held digest data and the transmitted digest data, and authenticates the application when the result of the collation is normal.

Claim 18 (New): A terminal connected fixedly or detachably to a secure device which holds data used by an application operated on the terminal, verifies validity of running unit configured to run the application, verifies validity of the application using digest data of the application calculated by the running means, validity of which is authenticated, accepts access by the application to the data when the validities of the running means and the application are authenticated, the terminal comprising:

    the running unit configured to run the application;

    application recording unit configured to record the application which is operated on the terminal and performs processing using the data held by the secure device; and

    recording unit configured to record the running means which runs the application,

    wherein the running means calculates the digest data of the application and sends the digest data to the secure device when the running means is authenticated by the secure device.

Claim 19 (New):   The terminal according to claim 18,
wherein the running means calculates the digest data after
the application requests to use the data held by the
secure device.

Claim 20 (New):   The terminal according to claim 18,
wherein the running means is recorded in an unwritable
area in the terminal, in which information are never
rewritten by the operation on the terminal device, and the
access from an external device.

Claim 21 (New):   An authenticating method used in a
secure device which is fixedly or detachably connected to
a terminal which includes running unit configured to
running an application, the method comprising:
     providing, in the secure device, data holding unit
configured to hold data used by the application which is
operated on the terminal, verifying unit configured to
perform authentication, and accepting unit configured to
accept access to the data;
     verifying validity of the running means by the
verifying means;
     calculating digest data of the application and
transmitting the digest data to the verifying means if the

validity of the running means is authenticated by the

verifying means;

verifying validity of the application on the terminal

by the verifying means using the transmitted digest data;

and

accepting, by the accepting means, access from the

application to the data held by the data holding means

when the validities of the running means and the

application are authenticated.

Claim 22 (New): An application authentication system

comprising:

a secure device for managing data used by an

application; and

running unit configured to run a Basic Input Output

System (BIOS), an Operating System (OS) operated on the

BIOS, executing software operated on the OS and executing

the application, and the application,

wherein the secure device verifies validity of the

BIOS,

wherein the BIOS verifies validity of the OS after the

verification by the secure device,

wherein the OS verifies validity of the executing

software after the verification by the BIOS,

wherein the executing software performs at least a part of processing of verifying validity of the application after the verification by the OS, and

wherein the secure device allows the application to use the data after the validity of the application is verified.

Claim 23 (10): The application authentication system according to claim 22, wherein

the application transmits a command to the secure device after the validity of the application is verified by the executing software, and

the secure device accepts the command only when the verification of the validity of the application is successful.

Claim 24 (New): The application authentication system according to claim 22, wherein

the executing software transmits information including a Hash of the application to the secure device, and

the secure device verifies validity of the information including the Hash of the application.

Claim 25 (New): A method used in a system having a secure device for managing data used by an application, and

running unit configured to run a Basic Input Output System (BIOS), an Operating System (OS) operated on the BIOS, executing software operated on the OS and executing the application, and the application, the method comprising:

verifying validity of the BIOS by the secure device;

verifying validity of the OS by the BIOS after the verification by the secure device;

verifying validity of the executing software by the OS after the verification by the BIOS;

performing at least a part of processing of verifying validity of the application by the executing software after the verification by the OS; and

allowing the application to use the data by the secure device after the validity of the application is verified.